ISSN 2754-1118

# IEC 61508 Viewpoint on System Safety in the Transport Sector

## Part 1 – An Overview of IEC 61508

**Derek Fowler**

Independent Safety Engineering Consultant, Reading, UK

## Abstract

*IEC publication 61508 "Functional safety of electrical/ electronic/programmable electronic safety related systems" is probably the most widely accepted, international generic standard on functional safety. Although its roots can be traced to process industries, the intention behind the Standard has always been to provide a solid, comprehensive basis for adaptation to a wide range of industry sectors. Nevertheless, previous published research into safety engineering practices in the transport sector has shown that, in some areas, those practices have failed to recognise even some of the most basic principles of IEC 61508 (as set out in Parts 1 and 4 of the Standard) and, as a consequence, focussed far more on the reliability of safety-related systems, and not enough on their potential risk-reduction properties. This paper, which is to be published as a series of parts, starting with this overview document (Part 1), will explore how IEC 61508 could be applied directly to the transport sector, with substantially beneficial results. No attempt is made to compare those results with actual practices in the specific transport applications addressed in Parts 2 and 3 – that is left to readers with a specific interest in those applications.*

# 1 Introduction

## 1.1 Background

IEC publication 61508 "*Functional safety of electrical/ electronic/programmable electronic safety related systems*" (IEC 2010) is probably the most widely accepted, international generic standard on functional safety. Although its roots can be traced to process industries, the intention behind the Standard has always been to provide a solid, comprehensive basis for adaptation to a wide range of industry sectors.

Using some simple principles from IEC 61508 as a benchmark, Fowler (2015) considered safety standards that were representative of practices in two transport-industry sectors — rail and aviation / air traffic management (ATM) — and found that, in some cases, they were "*wholly inadequate*" in that they focussed far more on the reliability of safety-related systems and not enough on their potential risk-reduction properties.

## 1.2 Aim and Objectives

The aim of this paper is quite different from, but complementary to, that of Fowler (2015). It seeks only to answer the simple question as to how, in the opinion of the author, the safety assessment of new (or significantly modified) systems deployed in specific transport applications would look if it followed, as far as practicable, the safety-specification phases of the lifecycle set out in Part 1 of IEC 61508, "IEC 61508-1". Any comparison of such an approach with current practices is left to the reader!

It is intended that the paper be issued in three parts, as follows:

**Part 1**, this document, whose objectives are to capture the essential principles that underpin IEC 61508, and show how those principles are embedded in the requirements-specification phases of the lifecycle set out in IEC 61508-1;

**Part 2** will describe, through a worked example, how the principles and lifecycle processes from Part 1 of the paper could be applied to European Air Traffic Management, and what the results would look like; and

**Part 3** will describe, through a worked example, how the principles and lifecycle processes from Part 1 of the paper could be applied to European rail transport, and what those results would look like.

## 1.3 Scope

The overall scope of the paper is deliberately limited to the safety-requirements specification phases of the IEC 61508 lifecycle. This is because most of the key principles underpinning IEC 61508, i.e. those universal principles set out in Parts 1 and 4 of the Standard, which govern the determination of the required risk-reducing properties of safety-related systems, take effect during these earlier phases, whereas the subsequent realisation and operating phases are less specific to the Standard.

Two important notes in IEC 61508-1, Sub-section 1.2, also have an impact on the scope of the discussions herein:

- Note 2: "*although a person can form part of a safety-related system (see also IEC 61508-4), human factor requirements related to the design of … safety-related systems are not considered in detail in the standard*";
- Note 4: "*although the overall safety lifecycle is primarily concerned with [electronic / programmable] safety-related systems, it could also provide a technical framework for considering any safety-related system irrespective of the technology of that system*".

## 1.4 Document Layout

After this introductory section, Section 2 of this document sets out the key concepts and principles upon which IEC 61508 is based.

Section 3 then outlines how these concepts and principles are applied in the safety-requirements-specification phases of the IEC 61508 lifecycle, using the simple example of a hypothetical pedestrian-crossing facility to illustrate the ideas behind them.

Semantics is vital to a clear understanding of IEC 61508; therefore, Appendix A hereto contains firstly a set of common safety definitions and, secondly, a set of terms that have a

particular meaning in relation to IEC 61508. Reference to a definition is given below thus: '[A.n-r]', where 'r' provides a hyperlink to the relevant item.

# 2 IEC 61508 Key Principles

## 2.1 Functional Safety Concepts

Functional safety [A.2-5], unlike "health and safety at work", is *[that] part of the overall safety relating to the EUC and the EUC Control System that depends on the correct functioning of the safety-related systems and other risk-reduction measures*.

Any safety assessment that accords with the key principles of IEC 61508 must start with the concept of the equipment under control (EUC). The definition of EUC [A.2-1]: "*equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities*", gives an insight into how the idea of an EUC might be interpreted more broadly than its actual title might suggest; for example, the flow of traffic along a road (or roads), the movement of trains along railway track, and the flow of aircraft through a portion of airspace, might all be thought as being an "EUC", and such a broader interpretation is not prohibited by the above definition. Whatever form the EUC takes, its essential property is that it is inherently hazardous!

An EUC Control System is defined as "*that system which responds to input signals from the [EUC] and/or from an operator, and generates output signals causing the EUC to operate in the desired manner*" [A.2-3]. Examples from the transport sector are road-vehicle control systems (including the driver, if not fully automatic), railway-signalling systems and air-traffic control systems. It could be an integral part of the EUC or a separate system and could, if it made a significant contribution to the safety of the EUC, be considered to be a safety-related system [A.2-10] in its own right.

From a safety perspective, two crucial points need to be born in mind:

- firstly, it is the EUC, together with its Control System, which lies at the heart of the IEC 61508 safety assessment process, since it is the (unmitigated) risk caused by the very existence of the EUC, for which safety functions [A.2-7] [A.2-9] need to be provided in order for the EUC Risk [A.2-4] to be reduced to a Tolerable level [A.1-5]; and
- secondly, whether an overall functional system is safe or not depends not just on its own inherent properties but also on the parameters of the Environment [A.2-2] —including, for example, physical, operating, legal and maintenance environments — in which the system is deployed.

## 2.2 Risk Reduction Overview

The principle of risk reduction is illustrated first of all in Figure 1, which is a generalised risk model, adapted from Figure A.1 of Part 5 of IEC 61508, "IEC 61508-5".

In the definition of EUC Risk [A.2-4], Note 4 emphasises that the "*main purpose of determining the EUC Risk is to establish a reference point for the risk without taking into*

*account* [the possible risk reduction afforded by] *any Safety-related Systems or any other risk-reduction measures*"[1].

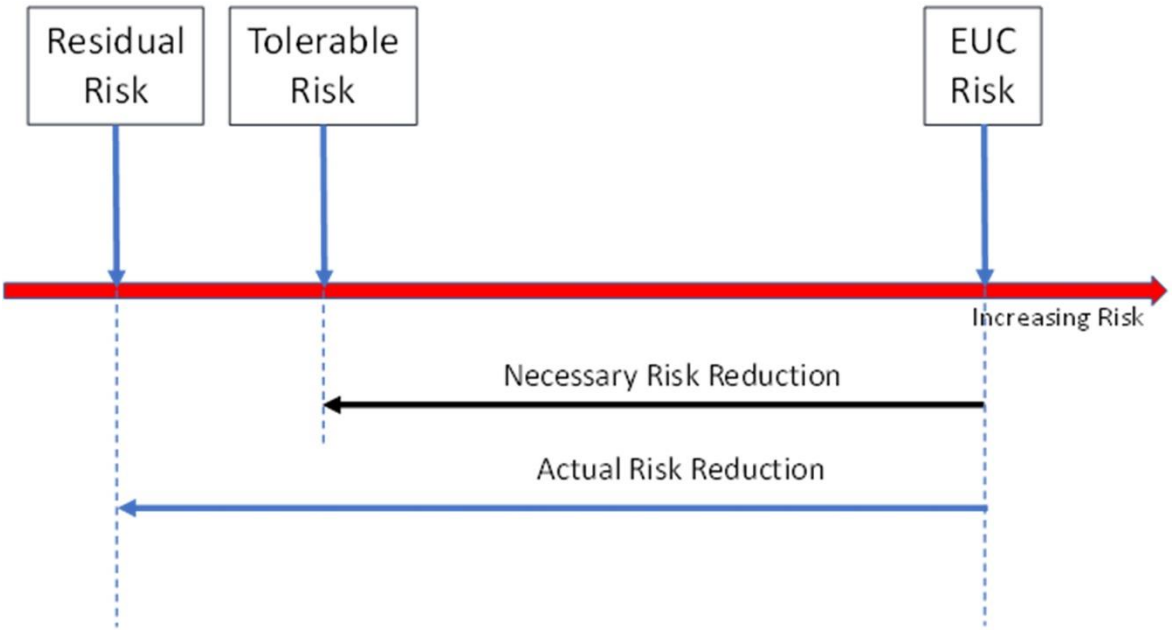


**Figure 1 ~ Basic Risk Model**

Necessary Risk Reduction (NRR) [A.2-6] is then the risk reduction that *must* be achieved by the Safety Functions in order to ensure that the Tolerable Risk is not exceeded, for a given level of EUC Risk.

Residual Risk [A.2-8] is the risk that is *actually* achieved for the specified hazardous events for the EUC / EUC Control System, but with the risk reduction afforded by the safety functions now taken into account[2].

## 2.3 Safety Integrity

We now need to address the question as to where Safety Integrity (i.e. "*the probability of a … safety-related system satisfactorily performing the specified safety functions under all the stated conditions, within a stated period of time*" [A.2-11]) fits into the picture.

This is illustrated in Figure 2 and, whereas this diagram is not presented explicitly in IEC 61508, it follows logically from the above, as follows.

First of all, we have introduced the idea of a maximum possible amount of risk reduction, $\delta R(max)$ — relative to the EUC Risk ($R_{EUC}$) — which applies in the hypothetical case of a set of Safety Functions, implemented in safety-related systems (SRSs) and/or in other risk-reduction measures (ORRMs), which are entirely failure free. Clearly $\delta R(max)$ cannot be related to safety integrity since we have, in effect, assumed the latter property to be 100%. Therefore, the (hypothetical) maximum amount of achievable risk reduction must be dependent solely on what the safety functions do (i.e. their functionality) and on how well they do it (i.e. their performance); furthermore, the resulting minimum achievable risk ($R_{MA}$)

[1] In *practice*, we will see that it is not always essential (or possible) to determine an absolute value of EUC Risk *provided*: all of the hazardous events associated with the EUC, and its operational environment, are identified, appropriate safety functions are specified, and the residual risk can be shown to be less that the relevant tolerable risk.

[2] Note that, in this illustration, we are in the fortunate position of achieving an actual level of overall risk reduction that is below that which is necessary for a safe state to be achieved overall.

is generally taken to be non-zero on the basis that there would always be some EUC hazardous situations that the safety functions would not be able to mitigate fully.

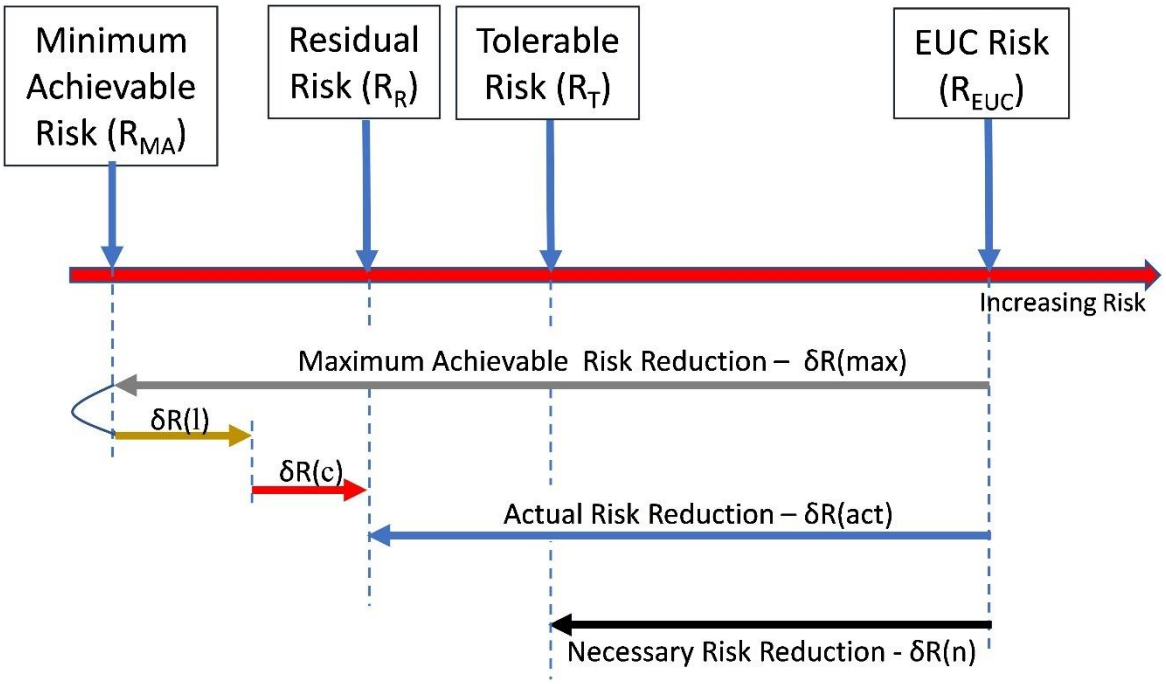


**Figure 2 ~ Safety Integrity Concepts**

Then we have δR (l), which represents an increase in risk arising from 'loss-type' failures of one or more safety functions; it is not a new risk as such — rather, it is effectively a shortening of the maximum achievable risk reduction arrow (i.e. a reduction below δR(max)).

δR(c), on the other hand, is a new source of risk because it arises from corrupt behaviour – i.e. incorrect or spurious operation — of one or more safety functions. Hence the Actual Risk Reduction is given by:

$$\delta R(act) = \delta R(max) - \delta R(c) - \delta R(l) \qquad \text{……(1)}$$

The inescapable conclusion from Equation (1) is that, in order for the residual risk ($R_R$) to be no higher than the tolerable risk ($R_T$), the tolerable maximum rates of loss and corruption failures for the safety functions cannot be determined in isolation from the amount of necessary risk reduction (δR(n)) that the safety functions are required to provide in the first place.

In other words, carrying out a safety analysis of safety-function failures cannot, in itself, tell us if a state of tolerable risk would exist for the system as a whole (i.e. the EUC, EUC Control System, and SRSs) and, in order to determine the safety integrity required of the safety functions, we must first assess, under assumed failure-free conditions, the potential minimum achievable risk ($R_{MA}$) that the safety functions could provide, in relation to the EUC Risk ($R_{EUC}$)[3].

[3] This conclusion has, as explained further in Fowler (2015), serious implications for safety-assessment methodologies that, in effect, focus almost entirely on the analysis of safety function (or, at a lower-level SRS) failure — including in the Air Traffic Management and Rail sectors.

## 2.4 Safety Integrity Levels and Safety Assurance

A safety integrity level (SIL) is defined by IEC 61508-4 as follows [A.2-12]:

> *"…discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest".*

Note 3A to this definition emphasises that a SIL "*is **not** a property of a system, subsystem, element or componen*t". This begs the questions as to what SILs actually are, and what they are for; to answer these, we next need to consider some basic principles of safety assurance.

IEC 61508 does not provide an explicit definition of safety assurance although, as we will see, it is certainly implicit in many parts of the Standard.

A useful definition of safety assurance, derived from European law (Commission Regulation (EU) No 1035/2011), is as follows (European Commission 2011):

> [A compelling argument supported by the body of evidence resulting from the application of*]*[4] "*all planned and systematic actions necessary to afford adequate confidence that a product, a service, an organisation or a functional system achieves acceptable, or tolerable, safety".*

"Confidence" is the operative word here and SILs play an important part in giving that confidence, to a level *appropriate to the risks involved*, by:

- setting standards for the design of products used in Safety-related Systems; and
- ensuring that an appropriate level of rigour is applied to the processes followed throughout the development, manufacture, operation, and maintenance of Safety-related Systems.

The manner in which SILs are *applied* is largely covered by Parts 2 and 3 of IEC 61508 and related to Phase 10, *et seq*., of the lifecycle, i.e. outside the scope of this paper. What we *are* concerned with herein is the way in which SILs are derived in the first place, as follows.

## 2.5 Derivation of SILs

IEC 61508 "*does not specify the safety integrity level requirements for any safety function, nor does it mandate how the SIL is determined*[5]". Nevertheless, we can set out some broad principles by using a fault tree representation of risk, as shown in Figure 3.

The fault tree is simply an alternative way of presenting the information in Figure 2, which is itself a refinement of Figure 1 and, hence, of Figure A.1 of IEC 61508-5 (IEC 2010).

In mathematical terms, the simple fault tree applies to a single Safety Function, in what IEC 61508-4 defines as "*a low demand mode of operation*". However, the author's intention here is not to detail a quantitative approach to SIL derivation — rather, it is to present the general logical relationships involved, from which we can deduce some sound principles for such an approach.

[4] The lead-in phrase has been added by the author to emphasise that assurance is an evidence-based activity and most of the "confidence" comes not from the actions *per se* but from the results thereof.

[5] See Note 2 to the Introduction of IEC 61508-4.

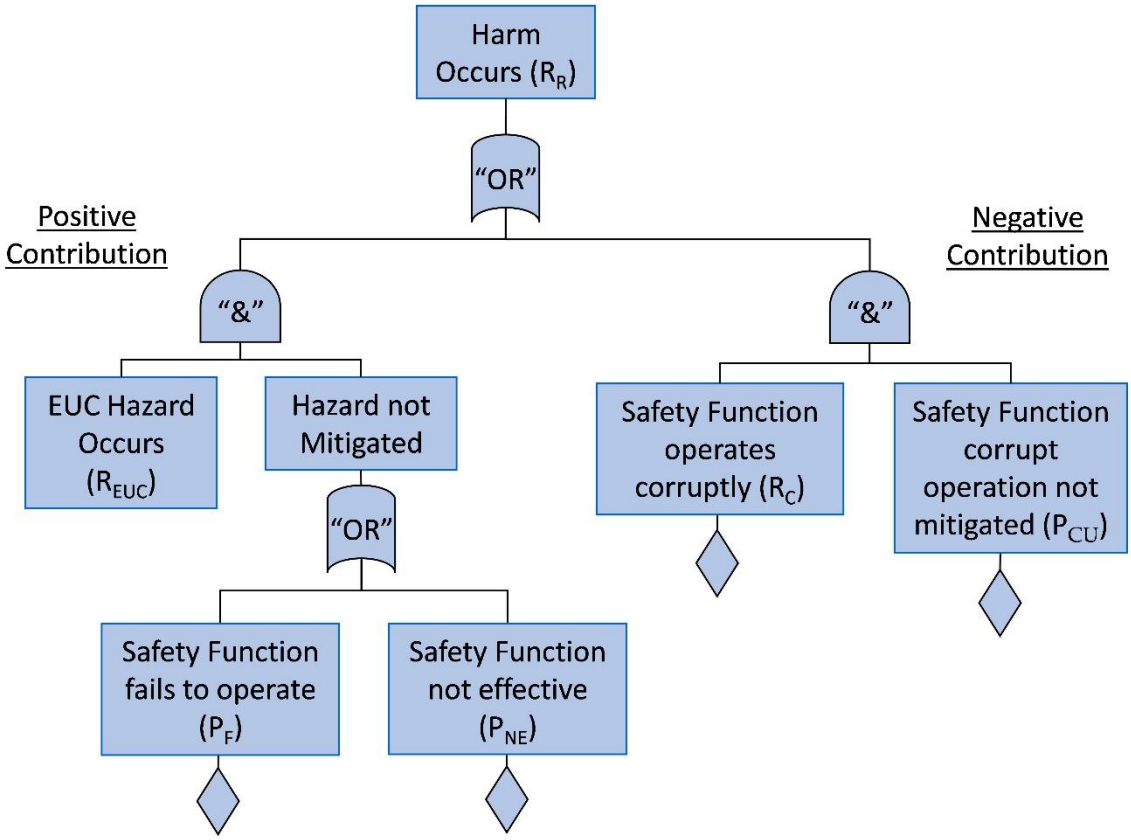


**Figure 3 ~ Fault Tree View**

In a general sense, a harmful event occurs if either:

- a hazard from the EUC occurs and is not mitigated by the Safety Function. Such a condition would occur if the Safety Function operated but was ineffective in mitigating the consequences of the EUC hazard under particular circumstances, or failed to operate at all; or
- the Safety Function operated corruptly, and the effects of this operation were not mitigated. Such a condition would occur if the safety function operated at the wrong time, under the wrong conditions, and/or in the wrong way, and if, for example, the corruption went undetected[6].

It is important to note again that the first of the above conditions is, in effect, the risk caused by failure to mitigate the EUC Risk, whereas the second condition is, in effect, a *new* risk that is not related to the EUC Risk.

As with most fault trees, Figure 3 can be used in a number of ways but if we were to *estimate* values (of probability or frequency, as appropriate) for the bottom-level events on each branch, *and* for the severity of the EUC hazard[7], we would end up with an estimate of risk for the top-level, harmful event.

Hence, relating Figure 3 back to Figure 2, we can see that:

[6] In neither case has the mitigating effect of Providence. i.e. the pure chance that a Hazardous Event or Hazardous Situation does *not* lead to a Harmful Event, been included in this simple model. In aviation for example, where the trajectory of an aircraft in flight has three degrees of freedom, Providence usually makes a major contribution to mitigating the consequences of a hazard; in the road and rail transport sectors, fewer degrees of freedom usually mean a lower contribution from Providence.

[7] If we wanted to model the likelihood of a range of hazard-severity outcomes, one way of so doing would be to connect the top-level risk to an Event Tree. That level of detail is, however, not necessary for the purposes of this paper.

1. in general, the top-level risk would equate to the residual risk ($R_R$);
2. if we were to set $P_F$ to 1.0 (i.e. a 100% probability that the safety function would have failed totally), then the top-level risk would become the EUC Risk ($R_U$)[8];
3. the difference between items 1 and 2 would equate to the actual risk reduction ($\delta R(max)$);
4. if $R_C$ and $P_F$ were set to zero, then the top-level risk would become the minimum achievable risk ($R_{MA}$); and
5. the difference between items 1 and 4 would equate to the sum of the risk due to the event "safety function failure to operate" ($\delta R(l)$) and the risk from "safety function corrupt operation" ($\delta R(c)$).

So, returning to the question of how to derive a SIL for the safety function, and referring to Figure 3, we know that EUC Risk ($R_{EUC}$) is (by definition) the risk which pertains when *no* safety function is in place, and can be represented by setting $P_F$, i.e. the probability of failure on demand for the safety function, to a value of unity on the fault tree. Note that, by setting $P_F$ to unity, we would effectively render the other base events irrelevant and, therefore, we would *not* need to know anything about $P_{NE}$, $R_C$ or $P_{CU}$ for this purpose. Given a reasonably accurate estimate for $R_{EUC}$, it would then be reasonably straightforward to compute a value for $P_F$ that would be required in order to *reduce* the top-level risk ($R_R$), from the level of the unmitigated EUC Risk, down to a tolerable level. That said, there are two important caveats to note here, as follows.

Firstly, for any value of $P_F$ *other* than unity, the other base events are not irrelevant, leaving us with two choices:

- to try to estimate values for $P_{NE}$, $R_C$ and $P_{CU}$; or
- redefine the computed value of $P_F$ such that it subsumes, into a single measure, the likelihood of all three possible causes of failure of the safety function — i.e. total loss, ineffectiveness (under specific circumstances), and corrupt behaviour.

The former option would probably not be viable since it would require considerably more detail about the safety function than would normally be available at this stage.

Fortunately, it turns out that the value of $P_F$ defined as above is synonymous with what IEC 61508 terms the "*target failure measure*" [A.2-13] for the safety function, and Table 1[9] below shows the four SIL levels together with their corresponding bands of target failure measures, for what IEC 61508-4 defines respectively as "*high demand*" and "*low-demand*" modes of operation.

Therefore, it would be a simple matter to look up the estimated value for $P_F$ in Table 1 – in this case the third column[10] – and read off the corresponding SIL.

Secondly, estimating a value for EUC Risk can be quite difficult for any safety-related application, not the least for the transport sector. However, IEC 61508-1, Sub-section 7.5.2.4 (IEC 2010) allows for an alternative way of deriving target failure measures that does *not* depend on direct knowledge of the unmitigated EUC Risk – this is discussed further in Phases 4 and 5 below.

[8] Values for $F_C$ and $P_{NE}$ are not relevant here because the of EUC Risk is defined as being the risk pertaining in the complete absence of the safety function – this is represented fully by simply setting $P_F$ to unity.

[9] Table 1 herein simply combines Tables 2 and 3 of Sub-section 7.6.2.9 of IEC 61508-1 (IEC 2010).

[10] That is because Figure 3 applies specifically to a "low-demand" case; however, the same principle would apply to a high-demand situation.

**Table 1 ~ Target Failure Measures & Safety Integrity Levels (SILs)**

| SIL | Average frequency of a dangerous failure of the safety function per hour | Average probability of a dangerous failure on demand of the safety function |
|---|---|---|
| 4 | $\geq 10^{-9}$ to $< 10^{-8}$ | $\geq 10^{-5}$ to $< 10^{-4}$ |
| 3 | $\geq 10^{-8}$ to $< 10^{-7}$ | $\geq 10^{-4}$ to $< 10^{-3}$ |
| 2 | $\geq 10^{-7}$ to $< 10^{-6}$ | $\geq 10^{-3}$ to $< 10^{-2}$ |
| 1 | $\geq 10^{-6}$ to $< 10^{-5}$ | $\geq 10^{-2}$ to $< 10^{-1}$ |

# 3 IEC 61508 Lifecycle Processes

## 3.1 Overview

This section explains how the above IEC 61508 principles are applied throughout the related phases of the IEC 61508 lifecycle.

Figure 4 shows the *overall* processes involved in the specification and realisation of the safety properties required by the SRSs and ORRMs in order that a tolerable level of risk could be achieved for the EUC / EUC Control System.

The diagram is based on Figure 2 of IEC 61508-1 (IEC 2010), with the following modifications:

- items in grey are shown for context reasons only, and fall outside the scope of this paper;
- Phases 6 to 8 have been omitted entirely as they cover only the planning for Phases 12 to 14 respectively;
- a summary of the main outputs of each relevant phase has been added to the diagram;
- the specification of safety requirements for ORRMs, i.e. Phase 11, falls within the scope of this paper, even though it is outside the scope of IEC 61508 itself; and
- IEC 61508's use of the term "*E/E/PE (System) — Electrical/Electronic/Programmable Electronic (System)*" was felt to be too specific and limiting for the purposes of this paper; therefore, the more general term "safety-related system (SRS)" is used instead herein so as to allow human and procedural elements to be included as well as (and possibly instead of) technical equipment.

An outline of the various pertinent lifecycle phases is set out as follows. Where applicable, the relevant IEC 61508-1 sub-section number is given and, as far as possible, the text is taken directly from the Standard. However, in some cases it has been found necessary to modify, or add to, the 61508-1 text in order to clarify a particular point, or to cater for some of the additional complexities of the transport sector; wherever this is the case, the rationale for such changes is given.

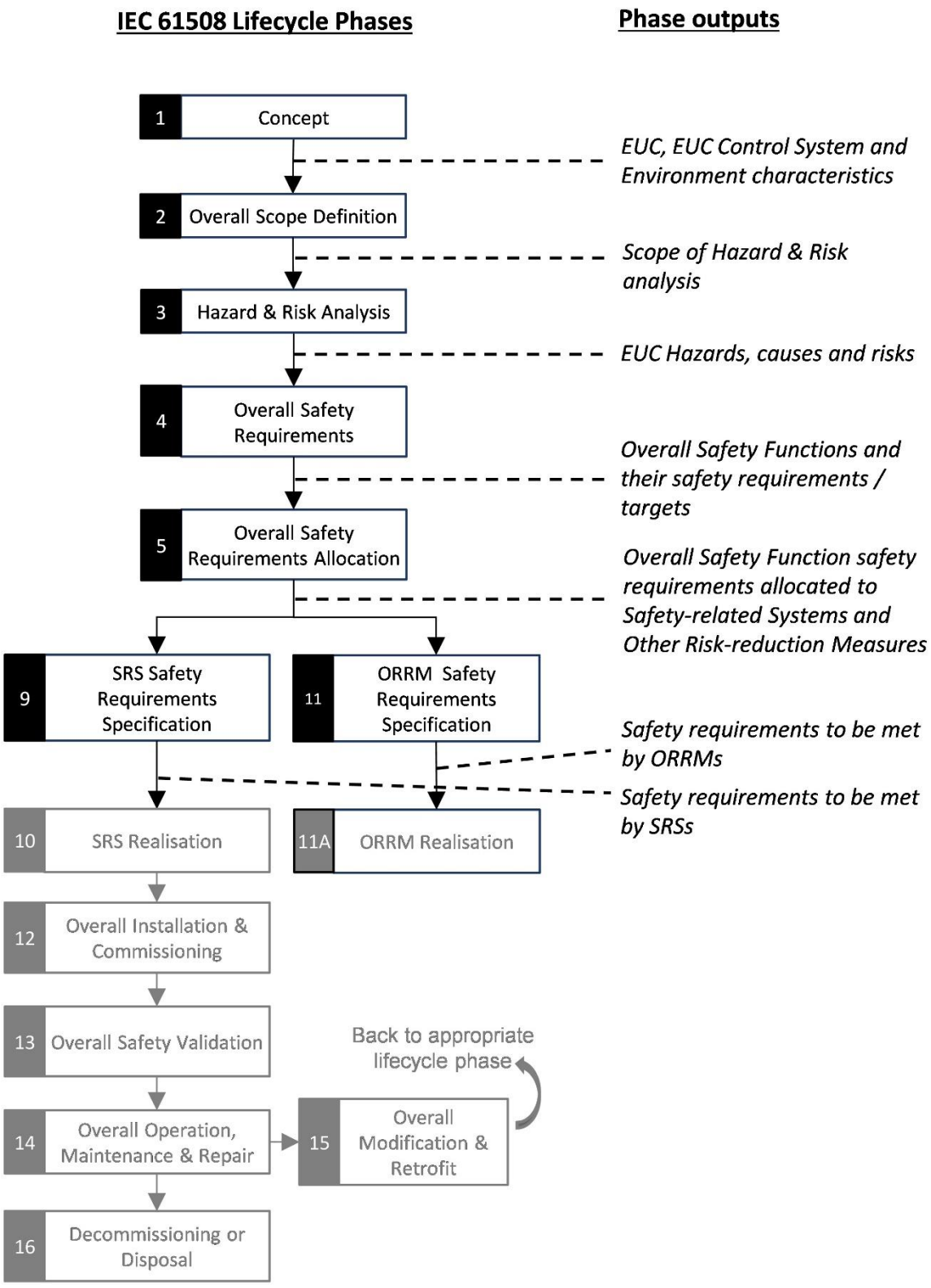


**Figure 4 ~ IEC 61508 Overall Safety Lifecycle**

For each lifecycle phase, guidance is given on the key issues involved in meeting the stated aim. Where applicable, this guidance is illustrated by considering a very simple, hypothetical road-transport application — the safety of pedestrians crossing a busy road[11]; however, unlike in subsequent parts of this paper, which will include more-detailed, worked examples, the discussion below is limited to highlighting the general issues involved in each phase, without seeking to resolve them for the specific case.

## 3.2 Phase 1: Concept (IEC 61508-1, Sub-section 7.2)

### *3.2.1 Aim*

The aim of this phase is to gather as much information about the EUC / EUC Control System and its environment as is necessary and sufficient to enable the other safety-lifecycle activities to be satisfactorily carried out.

It is important to note that, as an enabling activity, this would be a precursor to, but not form part of, the safety assessment *per se* and would require *substantial* operational and system-engineering specialist input, relevant to each specific application.

### *3.2.2 Guidance*

Section 4 of Fowler and Pierce (2012) explains the importance of the relationships involved here, in terms of good requirements-engineering practice. In essence, if we are to derive a valid set of safety requirements — initially for overall safety functions and, from those, for the corresponding SRSs and ORRMs — we need to establish precisely those properties of the EUC / EUC Control System and environment that could impact on the overall safety functions and their ability to mitigate EUC Risk to the degree necessary.

To get the Phase 1 process underway, the first step would have to be to decide what the EUC / EUC Control System actually comprises — something that is not necessarily immediately obvious! For our pedestrian-safety problem, we might decide to define the EUC as the flow of road traffic in the area of potential conflict with pedestrians; the flow of pedestrians would then form part of the *operating* environment. The logic of that decision is that it is the road traffic that presents hazards to the pedestrians, *not* vice-versa.

Properties of the traffic that we would need to know would include the various types of vehicle using the road (cars, buses, vans, heavy goods vehicles, automated vehicles, cyclists, etc.), the relative numbers of each, and their flow rates at different times of the day or week.

Examples of properties of the environment are:

- the road layout (e.g. road width, visibility, number of traffic lanes, single or dual carriageway, one- or two-way traffic, and the width available for the passage of pedestrians), and typical weather conditions (*physical* environment);
- characteristics of any proximate facilities (schools, hospitals, transport hubs, etc.) that could affect the flow of pedestrians at different times of the day or week (*physical* environment);

[11] This is *purely* for the purposes of illustration. It is not suggested that that the safety assessment of a proposed pedestrian crossing would have to be carried out this way.

- pedestrian characteristics (age, capability / disability, etc. and the relative numbers of each), pedestrian behaviours (e.g. inclination to avoid being hit by vehicles and yet a tendency to take risks), and the crossing rate of pedestrians (*operating* environment);
- vehicle speed limits, rights of way, etc. (*legal* environment);
- potential roadworks (*maintenance* environment).

It is important to note here that there is an extant EUC Control System — i.e. the natural inclination (if not legal obligation!) of vehicle drivers to comply with traffic signs and signals, and to avoid collisions with pedestrians and other vehicles in the flow. Indeed, in many road environments, with low density of pedestrians and road traffic, the EUC Control System would probably be sufficient in itself to achieve a tolerable level of risk of harm to pedestrians.

For more complex applications, e.g. ATM and rail systems, the EUC, EUC Control System, and environment would not only themselves be far more complex than the above and would, therefore, require much more detailed descriptions and analyses, but would also play a much greater part in the achievement of tolerable risk for the EUC (see the guidance on overall safety-function SIRs in Sub-section 3.5.2 below)[12].

## 3.3 Phase 2: Overall Scope Definition (IEC 61508-1, Sub-section 7.3)

### *3.3.1 Aim*

The aim of this phase is to define the scope of the hazard and risk analysis, for Phase 3.

### *3.3.2 Guidance*

Sub-section 7.3 of IEC 61508-1 starts this phase by determining the boundary of the EUC and the EUC Control System. The important issue here is that we are not trying to determine the actual limits of the EUC / EUC Control System, or of its environment, in absolute terms, since that should have been done in Phase 1 — rather, the requirement here is to decide the boundaries purely of the analysis work, in terms of the EUC / EUC Control System and its environment, as appropriate to the overall safety functions(s) that we are wanting to specify.

For example, for the hazard and risk analysis associated with our pedestrian-safety problem, we might want to:

- limit the hazards for pedestrians to those occurring only within a designated crossing area;
- exclude hazards not caused by the traffic; and
- exclude vehicle-vehicle collisions and vehicle incursions into pedestrian-only areas.

IEC 61508-1, Sub-section 7.3.1 helpfully notes that "*Several iterations between the overall scope definition and the hazard and risk analysis* [Phase 3] *may be necessary*"!

[12] That will also become increasingly true in road transport with the advent of automated vehicles.

## 3.4 Phase 3: Hazard and Risk Analysis (IEC 61508-1, Sub-section 7.4)

### *3.4.1 Aim*

The aim of this phase is to determine and characterise all the hazards and risks associated with the EUC / EUC Control System in the stated operational environment, within the scope identified in Phase 2.

### *3.4.2 Guidance*

It is vital to understand that, at this stage, the *subject* of the hazard and risk analysis is the EUC and its control system, *not* the overall safety function(s) or SRSs, which come later in the process. IEC 61508-1, Sub-section 7.4.1, Note 1, stresses this point as follows:

> *"This subclause is necessary in order that the safety requirements for the … safety-related systems are based on a systematic risk-based approach. This cannot be done unless the EUC and the EUC Control System are considered".*

Regrettably, this fundamental point does not seem to be widely understood — at least not in some key areas of the transport sector — as discussed in Fowler (2015).

Sub-section 7.4.1 of IEC 61508-1 identifies the following three distinct steps in the hazard and risk analysis process.

**Firstly:** to determine the hazards, hazardous events and hazardous situations relating to the EUC and the EUC Control System, in all modes of operation, and for all reasonably foreseeable circumstances — principally normal, abnormal, and failure conditions.

This requires that the hazards, hazardous events, and hazardous situations of the EUC and the EUC Control System be determined under all reasonably foreseeable circumstances, including fault conditions, reasonably foreseeable misuse, and malevolent or unauthorised action. It must include all relevant human factor issues and must give particular attention to abnormal, or infrequent, modes of operation of the EUC.

The main EUC hazard of interest for our pedestrian-safety problem is probably the *hazardous situation* that:

> *Haz #1: the respective needs of the traffic flow (EUC / EUC Control System) and the flow of pedestrians result in the moving traffic and pedestrians intending to occupy the same area of the road surface at the same time.*

It might also be relevant to consider two additional hazards, which could arise from failure of the EUC Control System and in the environment, respectively:

> *Haz #2: failure of a vehicle driver to take action to avoid a stray pedestrian;*
> *Haz #3: failure of a pedestrian to notice an on-coming vehicle.*

Specific IEC 61508 requirements on EUC Control System failures are explained in Phase 5 (Sub-section 3.6.2) below.

**Secondly:** to determine the preconditions and sequences leading to the hazardous events and hazardous situations.

This step is important in that knowledge of what causes or leads to hazardous events or situations can itself:

- lead to a clearer understanding of how such events or situations could be avoided — i.e. the hazard eliminated — sometimes the preferred solution; and/or
- facilitate estimation (in step 3) of how frequently such events or situations would be likely to occur.

Automatic traffic counters would be a typical means of collecting overall road-usage data on the vehicle flows around the area of interest for our pedestrian-safety problem. These could be supplemented by more selective techniques such as on-site enumerators or video cameras to collect pedestrian and cycle-survey data. It would also be useful to know:

- what determines the patterns of vehicle flows including what percentages of traffic is simply transiting the local area as opposed to requiring access to local facilities;
- about the presence of local facilities that could have a particular impact on pedestrian and/or vehicle flows, i.e. schools, workplaces, shopping centres, bus stops, etc.

**Thirdly:** to determine either the EUC Risks associated with the hazardous events and hazardous situations or the consequences of those events / situations.

This step might seem to be an essential condition for determining the NRR and thence the SIL and safety integrity requirements (SIRs), for each overall safety function. However, we will see in Phase 4 that IEC 61508-1 provides a means of avoiding the necessity of having to estimate EUC Risk, provided the consequences of the EUC hazards are known; we have, therefore, extended the original text of IEC 61508-1, Sub-section 7.4.1.3 to allow for this option.

It is not difficult to see that the estimation of EUC Risk depends heavily on information gathered in the preceding phases and processes, not the least of which is a thorough and complete understanding, from Phase 1, of the EUC, its control system, and its environment.

## 3.5 Phase 4: Overall Safety Requirements (IEC 61508-1, Sub-section 7.5)

### *3.5.1 Aim*

The aim of this phase is to produce a specification of the *overall safety requirements* — i.e. in terms of functional safety requirements and safety integrity requirements — for the overall safety function(s) in order to achieve the required level of functional safety.

### *3.5.2 Guidance*

The language of Sub-section 7.5 (and as we will see below, of Sub-section 7.6) of IEC 61508-1 can be quite difficult in places. In order to address this, it was decided to:

- use the term “functional safety requirements” (FSRs) herein, instead of paragraph 7.5.1’s “*safety functions* [sic] *requirements*”; and
- use the term “overall safety function(s)” instead of paragraph 7.5.1’s “E*/E/PE safety-related systems and other risk reduction measures*”, since we need to specify only the *overall* safety functions at this stage, not SRSs or ORRMs as they will be done later, in Phase 5.

Three process steps can be discerned from IEC 61508-1, Sub-section 7.5, as follows:

**Firstly:** to identify a set of overall safety functions, based on the EUC hazardous events derived from the hazard and risk analysis of Phase 3.

In the context of this step, Note 1 of IEC 61508-1, Sub-section 7.5.2.1, clarifies that: "*It will be necessary to create an overall safety function for each hazardous event*" associated with the EUC.

The importance of the word "overall" here is that the safety specification at this level is intended to be independent of whether the safety function would be realised as an SRS or ORRM (or both).

**Secondly:** to determine the required functional properties, i.e. the FSRs, of each overall safety function so as to address the related EUC hazard.

One way of achieving this is to start with wording of the related hazard and turn it into a high-level functional requirement statement of what needs to be done in order to mitigate the hazard — but *not* how this is to be done.

Taking our pedestrian-safety problem as an example, there are three quite different ways in which we could reduce EUC Risk — viz mitigate the hazard consequences, reduce the frequency of occurrence of the hazard, or remove the hazard completely — with markedly different realisations such as a controlled or uncontrolled pedestrian crossing, a road bypass, a footbridge or an underpass.

The main hazard (Haz #1 above) was about "…*moving traffic and pedestrians intending to occupy the same area of the road surface at the same time*". All we need to do, in order to remove the hazard, would be to negate at least one of the two conditions that define the hazard, so that we end up with the following simple functional requirement statement:

> *"FSR 1: In the area of potential conflict, the overall safety function shall ensure the safe separation of pedestrians and moving road traffic temporally and/or spatially".*

Such a requirement does not preclude any particular mitigation strategy or ultimate technological solution and yet is, at the highest level, sufficient in itself provided the associated required safety integrity requirements (SIRs) accompany it.

**Thirdly:** to determine the SIRs for each overall safety function so as to achieve a tolerable level of risk.

Sub-section 7.5.2.4 of IEC 61508-1 explains that the overall SIRs must be specified in terms of either:

- "*the risk reduction required to achieve the tolerable risk*"; or
- "*the tolerable* [EUC] *hazardous event rate so as to meet the tolerable risk*".

Note that this means that the SIRs at this level are not properties of the safety function to which they relate — whereas the overall functional safety requirements, derived in the previous step, specify what the overall safety function has to do (functionally), the SIRs for the overall safety function specify a target amount of EUC Risk *reduction* that the safety function has to provide in order to achieve a tolerable level of risk overall.

The latter of the above two bulleted options is a less-direct way of expressing required risk reduction but, as discussed in Sub-section 2.5 herein, is more pragmatic — especially in the transport sector. In order to determine the tolerable rate of occurrence of an EUC hazardous event, to meet the tolerable risk, we would need to know the consequences of the EUC hazardous event, in terms of the probability that occurrence of the event would result in the harm to which the tolerable risk relates. This could be done quantitatively or qualitatively,

aided by, for example, some form of hazard severity matrix / risk classification scheme that had been pre-defined for the particular application *and* for use at the EUC-hazard level; IEC 61508-5 provides general advice on a wide range of such techniques.

Further, in relation to the derivation of overall SIRs, where any reliance is placed on a possible contribution to achievement of tolerable risk that might be assumed (or actually specified) for the EUC Control System, it is also very important to note the provisions of Sub-section 7.5.2.5 of IEC 61508-1, which state that:

> *"If, in assessing the EUC Risk, the average frequency of dangerous failures of a single EUC control system function is claimed as being lower than $10^{-5}$ dangerous failures per hour then the EUC Control System shall* [itself also] *be considered to be a safety-related control system* [and] *subject to the requirements of this Standard".*

The Note to Sub-section 7.5.2.5 of IEC 61508-1 then goes on to clarify that whatever average frequency of dangerous failures is claimed for the EUC Control System function (i.e. if below $10^{-5}$ per hour), all the IEC 61508 requirements appropriate to the corresponding SIL would need to be met for the EUC Control System.

Finally of note is Sub-section 7.5.2.6, which discusses the case where failures of the EUC Control System place a demand on one or more SRSs and/or ORRMs, but where the intention is not to designate the EUC Control System as an SRS; it sets out a number of assurance requirements regarding the provision of data to support the rate of dangerous failure claimed for the EUC Control System, which in any event must not be lower than $10^{-5}$ dangerous failures per hour.

For our pedestrian-safety problem, we have already identified the EUC Control System as being the actions of pedestrians and vehicles to avoid each other, and that in areas of low pedestrian and traffic flows this can provide an adequate level of safety. What we also know is that this particular EUC Control System is non-linear, and its effectiveness diminishes substantially as the pedestrian and traffic flow rates increase. Therefore, great care would need to be taken in making any claims in regard to its safety properties.

## 3.6 Phase 5: Overall Safety Requirements Allocation (IEC 61508-1, Sub-section 7.6)

### *3.6.1 Aim*

The aim of this phase is to allocate to SRS(s) and/or ORRM(s), the functional safety requirements and safety integrity requirements, which were derived for the corresponding overall safety function in Phase 4.

### *3.6.2 Guidance*

The language of IEC 61508-1 is again slightly problematic in that it does not always distinguish between "safety function" and "overall safety function" (e.g. in Sub-section 7.6.2.9) and the relationship between safety integrity requirements, target failure measures. and SILs is not always as clear as it might be.

This author's understanding is that:

- the *safety integrity requirements* for each of the *overall safety functions*, which are being allocated to SRSs / ORRMs in this phase, are as described in Sub-section 3.5.2 herein, i.e.

they are either the risk reduction, or the tolerable EUC-hazard occurrence rate, to be achieved by the associated overall safety function;
- a *target failure measure* is the specific, inclusive safety-integrity property required of each SRS in order to satisfy the allocated *overall safety integrity requirement*[13], and from which the SIL for the safety function can be derived. It is specified as either: the average probability of a dangerous failure on demand of the safety function, for a low-demand mode of operation, *or* the average frequency of a dangerous failure of the safety function for a high-demand (or a continuous) mode of operation (IEC 61508-1, Sub-section 7.6.2.5); and
- the allocation of requirements from an overall safety function to SRSs could be done at the whole-SRS level or at the level of the constituent safety functions within the SRS.

Three process steps can be discerned from IEC 61508-1, Sub-section 7.6, as follows:

**Firstly:** to decide how the overall safety function for each hazard is to be implemented in terms of SRS(s) or ORRM(s) or a combination of the two, as appropriate. This is a relatively straightforward requirements-allocation process and the first of many further steps towards defining a solution to the top-level requirements of the overall safety function.

For our pedestrian-safety problem, we appear to have at least three main options:

- to install some form of pedestrian-control crossing in order to allow pedestrians and moving traffic to share the same road space but separate them temporally;
- to build a footbridge (or underpass) in order to separate pedestrians from traffic spatially; or
- restrict the volume of traffic using the road in question, providing a bypass for through traffic if necessary.

The first option is clearly an SRS but supported by ORRMs in the form of road markings, warning signs and possibly barriers; the second and third options would clearly be ORRMs since they are non-functional in nature.

It would make sense to introduce the *As Low As Reasonably Practicable*, "ALARP", principle — see IEC 61508-5 and HSE (2021) — at this stage in order to decide which of the above options should be adopted, since both the costs involved, and the risk reduction achievable, would probably be significantly different. This could be done qualitatively or quantitatively, albeit the latter would probably require the use of a socially acceptable Value of a Prevented Fatality (HSE 2018).

**Secondly:** to allocate the functional requirements contained in the specification for the overall safety function (i.e. the overall FSRs) to the designated SRS(s) and/or ORRM(s).

This is also relatively straightforward except that an important question at this stage might be whether more details could and should be decided for the options, e.g. what sort of pedestrian crossing (Zebra, Pelican, Puffin, Toucan, *et alia*) would best meet the functional and integrity requirements of the overall safety function, given the properties of the operational environment concerned?

**Thirdly:** to allocate the safety integrity requirements contained in the specification for the overall safety function (i.e. the overall SIRs) to the designated SRS(s) and/or its constituent safety functions, thence derive a *target failure measure* and an associated SIL for each SRS / constituent safety functions.

[13] See also the discussion on the Derivation of SILs in Sub-section 2.5 herein

IEC 61508-1 deliberately does not allocate overall SIRs to (nor derive target failure measures nor SILs for) ORRMs; however, it is likely that some equivalent to SILs would be necessary for ORRMs in some transport applications.

Allocation of overall SIRs to SRSs is not straightforward and the advice of IEC 61508-1, Sub-section 7.6.2.6, that the "*allocation of the safety integrity requirements shall be carried out using appropriate techniques for the combination of probabilities*" is less than helpful! The problem is that, at this level of abstraction, there is no technological basis for apportioning 'probabilities' between SRSs belonging to the same overall safety function.

In terms of SIL derivation, we have the additional problem that the lack of knowledge of their ultimate technological implementation also means that that it would not really be possible to show independence between SRSs (and/or between the constituent safety functions of an SRS) and, therefore, in line with IEC 61508-1, Sub-section 7.6.2.10, it would be necessary to assign to all SRSs / safety function the same SIL — i.e. the highest SIL of all the SRSs belonging to the same overall safety function[14].

It follows, therefore, that whereas there is some guidance on the processes required under this step in the discussion on the derivation of SILs, in Sub-section 2.5 herein, any results must be regarded as tentative and subject to confirmation at Phase 10, (SRS realisation) of the lifecycle. Alternatively, IEC 61508-1, Sub-section 7.5.2.3, has two helpful notes:

- Note 1, which states specifically that, "*some of the qualitative methods used to determine SILs in IEC 61508-5, Annexes E and F, progress directly from the risk parameters to the safety integrity levels — hence, in such cases, the overall SIRs are implicitly rather than explicitly stated because they are "incorporated in the method itself*"; and
- Note 5, which allows more-generally for situations where an application sector international standard exists that includes appropriate methods for directly determining the safety integrity requirements; it may be used to meet the requirements of this part of the Standard.

## 3.7 Phase 9: SRS Safety Requirements Specification (IEC 61508-1, Sub-section 7.10)

[Note that Phases 6 to 8 of IEC 61508-1 fall outside the scope of this paper]

### *3.7.1 Aim*

The aim of this phase is to develop further the safety requirements for the SRS identified in Phase 5, in terms of its FSRs and the SIRs, in order to achieve the required functional safety.

### *3.7.2 Guidance*

The above "aim" has been derived from the "objective" of IEC 61508-1, Sub-section 7.10.1, and is consistent with Sub-section 7.10.2.1, which states clearly that:

> *"The* [SRS] *safety requirements specification shall be derived from the allocation of safety requirements specified in* [Phase 5] *…".*

[14] IEC 61508-1, Sub-section 7.6.2.10 is actually about independence between safety functions *within* SRSs; however, the same reasoning could, and should, be applied also to independence *between* SRSs.

However, the phraseology has been altered somewhat, to remove apparent ambiguities, e.g. "*safety functions requirements*" becomes "*functional safety requirements*", i.e. FSRs. Furthermore, the term "safety function" is never used generically herein — instead, the formal IEC 61508-4 definitions, at Appendix A hereto, have been adhered to and are understood as follows:

- an "*overall safety function*" is the highest level of abstraction of the single set of SRSs and/or ORRMs that provides the complete response to a specific EUC Hazard; and
- a "*safety function*" is one of a number of functional entities implemented by an SRS.

The following, slightly-paraphrased, note from Sub-section 7.10.2.2 of IEC 61508-1, explains the purpose of the outputs of this phase of the lifecycle and their important relationship with the requirements derived in the previous two phases:

> *"Note: The objective is to describe, in terms not specific to the equipment, the* [required safety properties of the SRS(s)]. *The* [SRS Safety Requirements] *Specification can then be verified against the outputs of the 'overall safety requirements' and the 'overall safety requirements allocation' phases, and used as a basis of the realisation of the* [SRS]. *Equipment designers can use the Specification as a basis for selecting the equipment and architecture".*

Unfortunately, Sub-section 7.10.2.2 itself is less helpful in that it states that:

> *"The SRS safety requirements specification shall contain requirements for the safety functions and their associated safety integrity levels".*

Since SILs might already been allocated to the safety functions implemented by SRSs, in Phase 5[15], and the fact that — in any event — SILs are not system properties (see Note 3A to the definition of a SIL [A.2-12]), the broader term "*safety integrity requirements*", is used instead of the more restrictive term "*safety integrity levels*".

The following two process steps can be discerned from IEC 6150-1, Sub-section 7.10:

**Firstly:** to derive a full description of the SRS's required functional and performance properties — and its behaviour in relation to the EUC, EUC Control System and environment — that are necessary to achieve the required risk reduction (i.e. NRR).

Figure 2 herein shows that this reduction needs to be greater than the NRR in order to allow for the risk associated with loss failure of the safety function (δR(l)) and the risk associated with corrupt operation of the safety function (δR(c)). Therefore, the resulting SRS Safety Requirements Specification will need to be supported by analysis to show that the SRS is able to provide the required risk reduction under all normal, abnormal and failure states of the EUC, the EUC control system and the environment, as well as the transitions between those states.

Sub-section 7.10.2.6 of IEC 61508-1, in particular, places great emphasis on the need for a description of the workings of the SRS at a functional level, including:

- a description of all the safety functions, how they work together to achieve the required functional safety and whether they operate in low-demand, high-demand or continuous modes of operation;

[15] That does not mean that SIL derivation could not, if necessary, be repeated at this level of the requirements hierarchy; rather, the point is that it is not the most important consideration at this stage in the process.

- the required performance attributes of each safety function, e.g. timing properties and, for more data-intensive applications than possibly envisaged by IEC 61508, data accuracy, latency, refresh rate, and overload tolerance;
- all interfaces[16] that are necessary to achieve the required functional safety;
- all relevant modes of operation of the EUC;
- response of the SRSs to abnormal conditions that might arise in the EUC or its environment;
- all required modes of behaviour of the SRSs — in particular, its failure behaviour and the required response in the event of such failure.

The underlying point is clear: before we get into the SIRs for the SRS, we need to fully demonstrate the adequacy of the *FSRs* in satisfying the requirements for EUC-risk reduction, in the absence of failure of the SRS.

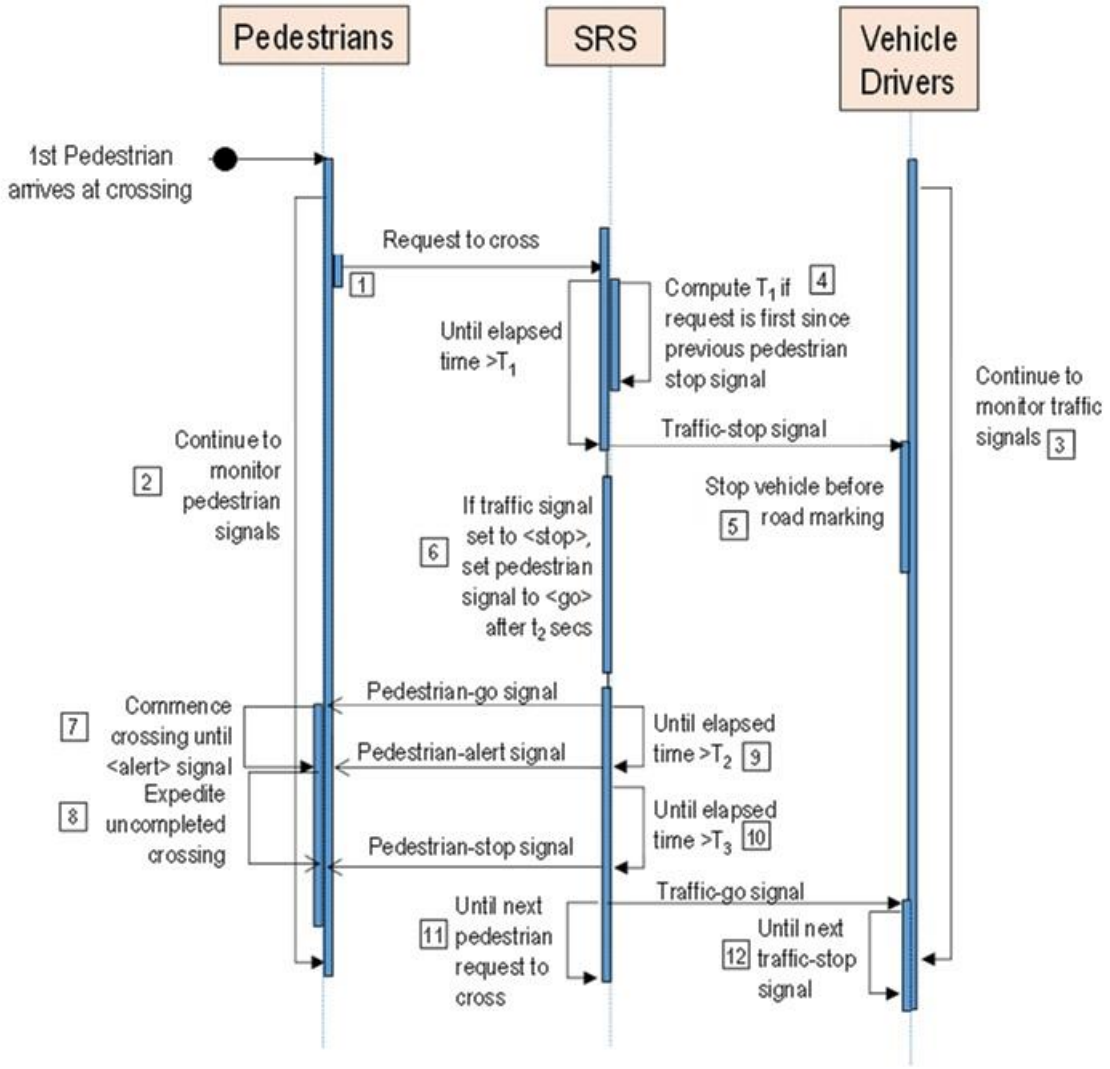


**Figure 5 ~ Sequence Diagram for the Pedestrian Crossing Example**

Assuming some form of temporal-separation solution and, given that the functionality is likely to be relatively straightforward, the FSRs specification for our pedestrian-crossing

[16] IEC 61508-1 also includes "operator" interfaces at this level. We have excluded that on the ground that human operators can by definition form part of a physical SRS and should be left until the physical (or at least logical) design stage of the development lifecycle.

could be based initially on the sequence diagram (Sparx Systems 2020) shown in Figure 5, as the main means of defining the logic and relationships involved for normal operational conditions.

A sequence diagram shows object interactions arranged in time sequence, represented by the vertical dimension. It depicts the objects (identified across the top) involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario.

Figure 5 represents a normal (or typical) scenario which starts when a pedestrian arrives at the crossing, during a period of road-traffic flow, and the sequence continues (for one iteration) as follows:

[1] the pedestrian initiates a request to cross;

[2] thereafter, pedestrians continue to monitor and comply with the pedestrian signals;

[3] vehicle drivers continue to monitor and comply with traffic signals;

[4] if the pedestrian request is the first request since the previous pedestrian <stop> signal, the SRS computes the time delay T1, else ignores the request;

[5] once the elapsed time since the pedestrian request to cross exceeds T1 then the SRS signals the traffic to <stop>;

[6] drivers stop vehicles before the appropriate road markings;

[7] after confirming that the traffic signal is set to <stop>, the SRS sets the pedestrian signal to <go> after a delay of T2 secs;

[8] pedestrians commence crossing until the crossing signal changes to <alert>;

[9] when the elapsed time since initiation of the <go> signal exceeds T3, the SRS sets the pedestrian signal to <alert>;

[10] at the <alert> signal, pedestrians already on the crossing complete their crossing expeditiously;

[11] when the elapsed time since pedestrian <alert> signal exceeds T4, SRS sets the pedestrian signal to <stop>;

[12] SRS maintains state until the next pedestrian request to cross;

[13] Traffic continues to flow until the next traffic <stop> signal.

The FSRs should capture the essence of the above scenario but in a more-formal language, starting with the overall functional requirement that pedestrian and traffic flows *shall* be controlled in turn such that pedestrians and moving traffic cannot occupy the designated crossing area at the same time. It should also include requirements that:

- call up the scenario itself as the required behaviour of the SRS;
- specify the time interval T1 (or its method of calculation) between the first crossing request by a pedestrian after traffic restart and the next instruction for the traffic to stop, such that there is a safe balance between the needs of pedestrians and the need to avoid excessive traffic queues;
- specify the total time interval T2 + T3 for which the traffic must be halted, such that it would be adequate to cater for the number and physical capabilities of pedestrians who might be using the crossing at the time;

- specify the time interval T3 such that pedestrians are given adequate warning of the imminent end of the crossing period;
- specify the means of indicating the state of the crossing to pedestrians such that it would be suitable for users with impaired hearing or vision;
- specify the default state of the crossing to be such that the traffic continues to flow in the absence of an input request from a pedestrian;
- specify that, under no circumstances, shall the pedestrian <go> signal and vehicle <go> signal states exist at the same time;
- specify the dimensions of the crossing area to be such that its pedestrian capacity would be great enough to handle the peak number of pedestrians under all reasonably foreseeable conditions.

The process of development of the FSRs would also need to address other, abnormal scenarios such as extreme weather and road maintenance which might affect the effectiveness of the SRS in providing the required risk reduction. Analysis should include assessment of the consequences and likely frequency of occurrence of such abnormal events so that account could be taken of the associated risk increase when developing the SIRs.

It is well worth noting here that sequence diagrams can be expanded, into greater detail, at lower levels in the system hierarchy — in the case of the pedestrian crossing shown in Figure 5, for example, by replacing the single "SRS" actor by the internal elements of its functional, logical and/or physical architecture — thus capturing the required behaviour at these levels, as required.

**Secondly:** to specify the detailed SIRs, for each safety function identified for each SRS, as follows:

- identification of the potential failure modes of the SRS(s), as well as the EUC control system;
- identification, and capture as additional FSRs, the possible mitigations of the frequency and/or consequences of those failures; and
- specification of the maximum occurrence rates of those failures, taking account of those mitigations, and of the minimum achievable risk that the SRS could provide, under assumed failure-free conditions[17], such that a tolerable level of risk for the EUC is achieved overall.

Thus far in the lifecycle, SIRs derivation has been largely deductive, "top-down", whereas it now needs to be inductive, "bottom-up". This is consistent with the note to the third step of Phase 4 (Sub-section 3.5.2 herein), that SIRs derived at the *overall safety function* level are *not* properties of the safety function itself.

It is also in line with commonly-accepted safety-assessment practices, and IEC 61508-5 suggests various techniques that could be used for this purpose — of course, any techniques and parameters involved must be demonstrably suitable for the application, and at the level in the requirements hierarchy, for which they are to be used.

It also needs to be understood that SIRs at this level would necessarily be based on an somewhat arbitrary apportionment of failure rates between the safety functions[18]; they would, therefore, need to be reviewed for the physical architecture of the SRS, at the

[17] See Sub-section 2.3 herein

[18] The nature of risk classification schemes, for example, means that they spread the target risk evenly across all failure causes.

realisation stage (Phase 10 in Figure 4) in order to avoid, for example, allocating inappropriately-low required failure rates to human operators.

### 3.8 Phase 10: Safety Requirements Specification for Other Risk-reduction Measures (IEC 61508-1, Sub-section 7.11)

IEC 61508 makes many references to ORRMs but otherwise rules them as outside the scope of the Standard — presumably as they are seen as being non-functional by nature. Therefore, since this paper is primarily about IEC 61508, albeit its potential application to the transport sector, it would not be relevant to introduce a lot of detail on ORRMs here.

Suffice it to say at this juncture that, whether they take the form of road, rail or runway layouts, or pre-defined routes through a block of airspace, ORRMs have a major role to play in the reduction of EUC Risk and, therefore, need to be treated, as far as possible, with the same (or equivalent) rigour as given to SRSs in IEC 61508. For example, in the case of a footbridge solution to our pedestrian-safety problem, it would be prudent to specify the relevant construction regulations.

## 4 Conclusions

Previous research, e.g. Fowler (2015), showed that, in some areas of the transport sector in Europe, some safety assessment practices, e.g. that of EUROCONTROL (2015) for ATM, and CENELEC (1999) for rail, focussed too much on system reliability and not enough on system functionality, contrary to, *inter alia*, the most basic principles of the international functional-safety standard IEC 61508 (IEC 2010).

This paper, to be published as a series in three parts, sets out to show what functional safety assessments for transport applications might look like if they followed the safety principles and lifecycle processes set out in IEC 61508-1 and IEC 61508-4. This first part gives an overview of those principles and lifecycle processes, together with some transport-orientated guidance, illuminated by applying it to a simple, hypothetical example of the assessment of a proposed means of enabling pedestrians to cross a busy road safely.

The scope of this exercise was limited to the seven lifecycle phases relating to the specification of safety requirements but, in so doing, showed that (subject to repeating it for more-challenging rail and ATM applications) it is not only possible to apply IEC 61508 to the transport sector but it also has the benefit of ensuring a correct balance in the approach to functional-safety assessment than might otherwise be the case.

The fundamental message at this stage is that the whole safety-assessment process must start with understanding the IEC 61508 concept of an EUC, and the hazards that it presents to its environment, *before* we can go on to specify the functional and integrity required of the Safety Functions, whose role is to mitigate the EUC hazards so as to achieve a tolerable level of risk overall.

As Fowler (2015) previously showed, not understanding this message can lead to safety-assessment practices that were wholly inadequate and, as recently as April 2021, the UK Transport Secretary (Grant Shapps) tweeted the following (Shapps 2021):

> *"85% of road accidents involve some element of human error. Today we're taking the first step towards self-driving* [sic] *cars on our roads making journeys safer …"*

Whether it was intended as a populist, or serious scientific, statement, the safety claim in the tweet is muddled thinking based on a serious *non sequitur*, as is the following related quote from the CEO of the Society of Motor Manufacturers and Traders, Mike Hawes (DfT 2021):

> *"Automated driving systems could prevent 47,000 serious accidents and save 3,900 lives over the next decade through their ability to reduce the single largest cause of road accidents — human error".*

According to UK Government statistics for the year ending June 2019, i.e. pre-COVID, there were "*1,752 reported road deaths, similar to the level seen since 2012*" (DfT 2020). To a first approximation, we could argue that, since about 1,450 of these deaths were due (at least in part) to human error, then replacing the human with more reliable automated driving systems would reduce the number of deaths caused by human drivers. However, the above two claims of an overall safety improvement would be true only if they took account of the countless millions of opportunities for fatal road accidents, i.e. the EUC Risk, which the skills and experience of the vast majority of human drivers have been amazingly successful in preventing. It follows, from the IEC 61508 principles and processes described herein, that the big challenge for the motor industry is to be able to show (with appropriate confidence and under all normal, abnormal and failure conditions) that the accident-*prevention* properties of automated driving systems (i.e. their safety functionality and performance) are also at least as good as those of the human drivers (part of the EUC control system) that they seek to replace — otherwise a huge increase in the number of road accidents might result.

Parts 2 and 3 of the series will consider the application of these ideas to ATM and rail systems.

## Acknowledgments

The author wishes to acknowledge the considerable help, support and understanding of IEC 61508 provided by his long-standing colleague Ronald Pierce, without which this paper would not have come to fruition.

The copyright holder of the quotations from published standards used for illustration in this paper is the International Electrotechnical Commission, Geneva.

## References

CENELEC. (1999). *Railway applications — the specification and demonstration of reliability, availability, maintainability, and safety (RAMS), Part 1: Basic requirements and generic process*, EN 50126-1, European Committee for Electrotechnical Standardization. Brussels.

DfT. (2020). *National Statistics — Reported road casualties Great Britain, annual report: 2019*. UK Government Department for Transport. Available at https://www.gov.uk/government/statistics/reported-road-casualties-great-britain-annual-report-2019. Accessed 19th June 2022.

DfT. (2021). *Government paves the way for self-driving vehicles on UK roads.* Department for Transport. Available at https://www.gov.uk/government/news/government-paves-the-way-for-self-driving-vehicles-on-uk-roads. Accessed 19th June 2022.

EUROCONTROL. (2015). *Safety Assessment Methodology, Version 2.2*. Available at https://www.eurocontrol.int/tool/safety-assessment-methodology. Accessed 19th June 2022.

European Commission. (2011). *Regulation (EU) No. 1035/2011 Laying Down Common Requirements for Provision of Air Navigation Services...* Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011R1035&from=EN. Accessed 19th June 2022.

Fowler D. (2015). *Functional Safety by Design – Magic or Logic?* In Proceedings of the 23rd Safety-Critical Systems Symposium, Bristol, UK. Available at https://scsc.uk/r129/7:1. Accessed 19th June 2022.

Fowler D, Pierce R. H. (2012). *A Safety Engineering Perspective*. In: Cogan B (editor) *Systems Engineering: Practice and Theory*. IntechOpen. London.

HSE. (2018). *Appraisal values or unit costs*. Health & Safety Executive. Available at: https://www.hse.gov.uk/economics/eauappraisal.htm. Accessed 19th June 2022.

HSE. (2021). *ALARP at a glance*. Health & Safety Executive. Available at: https://www.hse.gov.uk/managing/theory/alarpglance.htm. Accessed 19th June 2022.

IEC. (2010). *Functional Safety of Electrical/electronic/programmable electronic Safety-related Systems*, IEC 61508, V 2.0. International Electrotechnical Commission. Geneva.

Pierce R, Fowler D. (2010). *Applying IEC 61508 to Air Traffic Management*. In: Dale C, Anderson T (editors) *Making Systems Safer, Proceedings of the Eighteenth Safety-Critical Systems Symposium, Bristol, UK, 9-11th February 2010*. Springer-Verlag, London.

Shapps G. (2021, April 28). *Today we're taking the first steps towards self-driving cars on our roads*. Twitter. https://twitter.com/grantshapps/status/1387371484423786497. Accessed 19th June 2022.

Sparx Systems. (2020). *Message Examples*. Sparx Systems Pty Ltd. Available at https://sparxsystems.com/enterprise_architect_user_guide/15.2/model_domains/message_examples.html. Accessed 19th June 2022.

# Appendix A. IEC 61508 Safety Definitions

## A.1 General Definitions

The following are some well-understood, basic safety definitions, as set out in Part 4 of IEC 61508, "IEC 61508-4" (the notes from the standard are included); in each case, the normal English usage of the words used is intended to apply, unless stated otherwise:

1. "***Harm*** *– [death], physical injury or damage to the health of people or damage to property or the environment*";
2. "***Hazard*** *— potential source of Harm;*

   *Note: the term hazard includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long-term effect on a person's health (for example, release of a toxic substance)*";

3. "***Harmful Event*** *— an occurrence in which a hazardous situation or hazardous event results in harm;*

   *Note: harmful events can be considered to include accidents, although the latter are usually understood to be unintentional*";

4. "***Risk*** *— the combination of the probability of the occurrence of Harm and the severity of that Harm*";
5. "***Tolerable Risk*** *— risk that is accepted, in a given context, based on the current values of society*"; and
6. "***Safety*** *— freedom from unacceptable [i.e. intolerable] risk*".

## A.2 Functional Safety

In order to fully understand the notion of functional safety in the context of IEC 61508, we next need to deal with its (possibly off-putting[19]) definitions related to the so-called equipment under control (EUC) and introduce the concept of safety-related systems (again, the notes from the standard are included):

1. "***EUC*** *— equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities*";
2. "***Environment*** *— all relevant parameters that can affect the achievement of functional safety in the specific application under consideration and in any safety lifecycle phase;*

   *Note: this would include, for example, physical environment, operating environment, legal environment, and maintenance environment*".

[19] We will show that a broader, system view of that which is "under control" can be helpful in understanding how the essential principles of IEC 61508 can readily be applied to a diverse range of safety-related sectors.

3. "***EUC Control System*** *— system that responds to input signals from the* [EUC] *… and/or from an operator* [and /or from the EUC's operational environment[20]] *and generates output signals causing the EUC to operate in the desired manner*";
4. "***EUC Risk*** *— risk arising from the EUC or its interaction with the EUC Control System;*

*Note 1 The risk in this context is that associated with the specific harmful event in which E/E/PE safety-related systems and other risk reduction measures are to be used to provide the necessary risk reduction, (i.e. the risk associated with functional safety).*

*Note 2 The EUC Risk is indicated in Figure A.1 of IEC 61508-5. The main purpose of determining the EUC Risk is to establish a reference point for the risk without taking into account E/E/PE safety-related systems and other risk reduction measures*".

5. "***Functional Safety*** — [that] *part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the safety-related systems and other risk-reduction measures*".
6. "***Necessary Risk Reduction*** *— risk reduction to be achieved by the … safety-related systems and/or other risk reduction measures in order to ensure that the tolerable risk is not exceeded*";
7. "***Overall Safety Function*** *— means of achieving or maintaining a safe state for the EUC, in respect of a specific hazardous event*";
8. "***Residual Risk*** *— risk remaining after protective measures have been taken*";
9. "***Safety Function*** *— function to be implemented by a … safety-related system (qv)* [and/or] *other risk-reduction measures, which is intended to achieve, or maintain, a safe state for the EUC, in respect of a specific hazardous event*";
10. "***Safety-related System*** *— designated system that both:*

*- implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and*

*- is intended to achieve, on its own or with other safety-related systems and 'other risk-reduction measures', the necessary safety integrity for the required safety functions;*

*Note 1: The term refers to those systems, designated as safety-related systems, which are intended to achieve, together with the other risk reduction measures, the 'necessary risk reduction' (qv) in order to meet the required 'tolerable risk' (qv).*

*Note 2: Safety-related systems are designed to prevent the EUC from going into a dangerous state by taking appropriate action on detection of a condition which may lead to a hazardous event. The failure of a safety-related system would be included in the events leading to the determined hazard or hazards. Although there may be other systems having safety functions, it is the safety-related systems that have been designated to achieve, in their own right, the required tolerable risk ...*

*Note 3: Safety-related systems may be an integral part of the EUC Control System or may interface [directly] with the EUC …. That is, the required 'safety integrity level' (qv) may be achieved by implementing the safety functions in the EUC Control*

[20] The clause in brackets is not included in the IEC 61508 definition - we have added it for completeness, as part of the broader, system view of that which is "under control".

*System …. or the safety functions may be implemented by separate and independent systems dedicated to safety.*

*Note 4: A safety-related system may:*

*a) be designed to prevent the hazardous event (i.e. if the safety-related systems perform their safety functions then no harmful event arises); and/or*

*b) be designed to mitigate the effects of the harmful event, thereby reducing the risk by reducing the consequences* [of that event]*;*

*Note 5: Safety-related systems can be divided broadly into safety-related control systems and safety-related protection systems*"[21].

11. "***Safety Integrity*** *— probability of a … safety-related system satisfactorily performing the specified safety functions under all the stated conditions, within a stated period of time*".
12. "***Safety Integrity Level*** *— discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest;*

*Note 1 The target failure measures (see 3.5.17) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1.*

*Note 2 Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems.*

*Note 3 A safety integrity level (SIL) is not a property of a system, subsystem, element, or component. The correct interpretation of the phrase "SIL n safety-related system" (where n is 1, 2, 3 or 4) is that the system is potentially … capable of supporting safety functions with a safety integrity level up to n*".

13. "***Target Failure Measure*** *— target probability of dangerous mode failures to be achieved in respect of the safety integrity requirements, specified in terms of either:*

*– the average probability of a dangerous failure of the safety function on demand, (for a low demand mode of operation);*

*– the average frequency of a dangerous failure [h-1] (for a high demand mode of operation or a continuous mode of operation)*".

[21] In general, the former can be considered to maintain a continuous or continual safe state for the EUC whilst allowing the EUC to continue to execute its normal functions whilst the latter, when required, puts the EUC into a *safer* state even if this interrupts the normal functioning of the EUC